# Sociální inženýrství

V tomto modulu se seznámíme s typem bezpečnostních útoků, které pro své cíle bohužel využívají jednu z nejcitlivějších metod – psychologickou manipulaci, a to skrze naše přirozené lidské slabosti, tedy například **zvědavost, strach či nepozornost**. Skrze tento typ manipulace dokáže útočník svou oběť dokonale oklamat, ta se může následně dopustit bezpečnostní chyby a poskytnout tak útočníkovi informace v podobě citlivých údajů a přístupových práv, nebo rovnou peněžních částek. Přečtěte si příběhy lidí, kteří zažili některé z nejznámějších a nejčastějších technik sociálního inženýrství na vlastní kůži. Nemusíte se bát – nebudeme vás jen strašit, v každém z příběhů se dozvíte také rozuzlení a návod, jak se podobným děsivým scénářům vyhnout. Na těchto fiktivních příbězích chceme zejména ukázat, **jak dokážou být útočníci v kyberprostoru vynalézaví** a zákeřní, a co vše jsou ochotni využít, aby dosáhli svého cíle.

## Baiting

***Marie, 42 let***
**VEDOUCÍ UNIVERZITNÍ KNIHOVNY**

Marii považují její kolegové za zodpovědnou vedoucí univerzitní knihovny. Aby ne, v této pozici působí již deset let. Jednoho dne, cestou do práce najde Marie na parkovišti výrazně žlutý flash disk s nápisem „Teambuilding fotky“. Marie si takzvanou flashku chvíli prohlížela, a nakonec se rozhodla ji vzít. Leží přece před budovou, kde pracuje, a mohla by někomu chybět. Odnese ji na vrátnici a tam se o ni jistě přihlásí majitel. Po příchodu do kanceláře to ale Marii nedá. O jaký teambuilding asi šlo? A jaké zajímavé fotografie by tam mohla najít? Flashku vrátí, ale až si obsah sama prohlédne. Jedná se přeci o její kolegy, a kdyby ne, alespoň bude vědět, že nemá cenu disk na vrátnici odevzdat a vymyslí jiné řešení. Zapojí médium do svého pracovního počítače a otevře složku. Žádné fotografie však nenajde, jen nějaké nesmyslné soubory. Fotografie už asi někdo vymazal, pomyslí si. Škoda. Disk vytáhne a odnese jej na vrátnici budovy s úmyslem nahlásit nález.

Marie v tuto chvíli vůbec netuší, že se stala obětí takzvaného Baitingu – metody sociálního inženýrství, která využívá naši přirozenou zvědavost. Cílem útočníka v tomto případě bylo namotivovat lákavým popiskem na disku některého z pracovníků, aby médium zapojil do své pracovní stanice. Mezitím, co Marie hledala fotografie, se za jejími zády dávno spouštěl škodlivý software, který má možná nyní vládu nad jejím počítačem. Co s ním asi provede?

Marie má štěstí – má na svém pracovním počítači nainstalovaný a plně aktualizovaný antivirový program, který si se škodlivým softwarem poradí. Ne vždy to však končí takto.

|  |
| --- |
| **Pozor!** Nikdy do svých pracovních ani osobních zařízení nezapojujte a nevkládejte nosiče (flash disky, SD karty...), u kterých si nejste jisti původem a obsahem. Doporučujeme také svá zařízení zabezpečit: jak na to si ukážeme v pátém modulu. |

## Blagging

***Dominika, 32 let*MARKETINGOVÁ SPECIALISTKA**

*„Ahoj Domi! Prosím Tě, jsem ve velkým průšvihu! Jel jsem na služebku a ukradli mi peněženku, nemám se jak dostat zpátky domů. Mohla bys mi prosím přes tenhle odkaz poslat peníze na letenku? Prosím, zachraň mě! Petr.“*

Tento e-mail dostala hlavní představitelka příběhu o technice označované jako Blagging. Dominika v rychlosti přečetla zprávu, že se její kolega nachází v nesnázích, a samozřejmě chtěla ihned pomoci – Petr by pro ni přeci udělal to samé, ne? V reakci na urgentní situaci si ale nevšimla, že e-mail přišel z úplně jiné adresy, která neodpovídala Petrově pracovní či osobní adrese. Ve chvíli, kdy by Dominika odeslala peníze, stala by se obětí jedné z technik sociálního inženýrství. Metody, při které se útočník snaží zmanipulovat oběť zpravidla velmi poutavým a naléhavým příběhem.

U Blaggingu je velmi častý právě požadavek o určitou peněžní částku. Útok z našeho příběhu byl natolik sofistikovaný, že útočník využil reálnou identitu Dominičina kolegy. Jak věděl, že Petr opravdu vyrazil na služební cestu? Na výběr má přeci mnoho dalších technik sociálního inženýrství, které mohou k získání podobných informací posloužit! Co když Petr například sdílel veřejně fotku z ciziny na sociálních sítích? Útočníkovi pak stačí jen vymyslet poutavý příběh a zfalšovat e-mailovou adresu. Ale jak se proti Blaggingu bránit?

Pakliže obdržíte podobnou zprávu jako Dominika, **zkuste v první řadě ověřit adresu odesílatele**. Pakliže adresa odesílatele nesouhlasí s formátem adres vaší univerzity, je načase zpozornět.

|  |
| --- |
| **Pozor!** Nabudete-li podezření, kontaktujte danou osobu skrze **jiný komunikační kanál**, například osobní e-mailovou adresu, sociální sítě, anebo zkuste prostě a jednoduše dané osobě zatelefonovat. Potvrdí-li se vám, že se jedná o podvod, či daná osoba delší chvíli nereaguje, raději hlaste celý incident kompetentním osobám (IT technikům, vedoucím). V případě MUNI neváhejte situaci hlásit kyberbezpečnostnímu týmu <school-specific>. |

## Phishing

**Zdeněk, 38 let
VYUČUJÍCÍ FRANCOUZŠTINY**

Zdeněk se ve svém příběhu tváří v tvář setkává s nejrozšířenějším typem útoku sociálního inženýrství – phishingem. Phishing má zpravidla podobu v rozesílání hromadných podvodných e-mailů. Tyto podvodné e-maily se snaží z uživatele vymámit nejrůznější přihlašovací údaje. V osobním životě může jít o přihlašovací jméno a heslo k bankovnímu účtu, v zaměstnání zase o přístup do pracovních aplikací a systémů. V prostředí univerzity je to nejčastěji přístup do informačního systému. Co když ale útočníci změní taktiku a začnou si brousit zuby třeba na váš O365 účet <school-specific: použít kritický účet/identitu>? S takovým pokusem se setkal právě Zdeněk...

Zdeňkovi přišel v pátek odpoledne e-mail nabízející excelentní kurzy jazyků s výhodnými slevami v přiloženém dokumentu. Zaraduje se a přiložený soubor rozklikne. Náhle na něj vyskočí okénko s žádostí o oprávnění k přístupu ke Zdeňkovým údajům účtu O365. Požaduje přístup ke kalendáři, kontaktům a dalším položkám. Po odsouhlasení těchto požadavků by Zdeněk dal útočníkům plný přístup ke svému O365 účtu. Co by mělo být Zdeňkovi i vám, čtenáři, podezřelé na první pohled?

Při přistupování k jakémukoli souboru po vás O365 nikdy nebude chtít potvrdit přístup k účtu (ať seznamu kontaktů, změnám v kalendáři nebo čemukoli jinému). <school-specific>

Každá aplikace by vždy měla požadovat přístup pouze k položkám, které souvisí s její primární činností. Pokud Zdeněk otevírá odkaz na dokument ve Wordu z O365, proč by měla aplikace chtít přístup do jeho kalendáře nebo číst veškeré jeho soubory.

|  |
| --- |
| **Pozor!** Vždy si pečlivě přečtěte, jaké souhlasy aplikaci dáváte, i když myslíte, že ji „znáte jako vlastní boty“. Pokud se vám zdají požadavky podezřelé, či v případě, že phishingu podlehnete (což se vždy dříve nebo později projeví), nahlaste to.  |

## Pharming

**Štěpánka, 29 let
DOKTORANDKA**

Přestože se pharming může zdát ve svých důsledcích jako technika podobná phishingu <odkaz>, v reálném životě se s ním lze potkat méně často, vyžaduje totiž více práce ze strany útočníka. To ovšem neznamená, že bychom se před ním neměli mít na pozoru a stejně tak i doktorandka Štěpánka.

Štěpánka dnes jako každé pracovní ráno začala den přihlášením do Informačního systému kliknutím na záložku na liště svého prohlížeče. Záložku má na tento web v prohlížeči už roky, takže si v adresním řádku nevšimla podivné URL adresy, která se od obvyklé mírně lišila a nevědomky tak předala své údaje útočníkovi. Jak se to mohlo stát? Útočník možná napadl DNS server <slovník> univerzity a přesměroval Štěpánku na téměř identickou kopii přihlašovací stránky. Každý pharmingový útok ovšem nemusí být takto rozsáhlý a pokud by si útočník například brousil zuby na Štěpánčin přístup do bankovního účtu, mohl využít právě phishingu, aby následně pomocí nastraženého škodlivého softwaru při jejím příštím vstupu do internetového bankovnictví zobrazil až na pár malých detailů téměř identickou kopii přihlašovací stránky.

Co bychom tedy měli my (i Štěpánka) dělat, abychom odevzdání svých údajů předešli? Kromě dodržování zásad předcházejících phishingu je dobré kontrolovat v adresním řádku, zda se skutečně nacházíme na věrohodné stránce a nezanedbávat pravidelné antivirové kontroly. Tam, kde je to možné, se také vyplatí mít nastavené dvoufaktorové ověřování <odkaz na slovník> při přihlašování do dané webové aplikace.

## Spear-phising

**Jana, 24 let
EKONOMKA**

Spear-phishing lze nazvat sofistikovanějším bratrem phishingových technik. V čem spočívá jeho zákeřnost? To zakusí začínající ekonomka Jana... Každý z nás patří pracovně do určité skupiny s konkrétními právy a specifickými přístupy. Nejčastěji útočníky vyhledávanou skupinou jsou pracovníci, kteří manipulují s peněžními prostředky a vysoce citlivými daty. A právě Jana spadá do této skupiny.

Do pracovní e-mailové schránky jí denně přichází několik desítek zpráv. Dnes se mezi nimi objevila i zpráva, jež nesla název „*Kalendář plánu mezd listopad*“. Stručná zpráva mimo tohoto popisu obsahovala také odkaz, který vybízel k otevření dokumentu na příslušné adrese. Po kliknutí na odkaz se Janě na obrazovce objevila učebnicová phishingová stránka, která se snažila napodobit jednotné přihlášení do univerzitního systému <school-specific>. Ve chvíli, kdy by Jana tento formulář vyplnila, její přihlašovací údaje by putovaly přímo do rukou útočníka, který je může libovolně zneužít.

Proč měla Jana tendenci tento e-mail otevřít? Souvisel totiž přímo s její pracovní náplní, a právě na to útočníci sázeli. Mimo to se také mezi dalšími pracovními e-maily poměrně dobře zamaskoval. Co mohla Jana udělat, aby se ujistila, že něco není v pořádku? A čím se můžete řídit i vy?

I přes věrně působící vizuální identitu si vždy důkladně prohlédněte adresní řádek. Je všechno v pořádku? V každodenní rychlé pracovní rutině nezbývá tolik času na kontrolu každého detailu v e-mailu nebo na webu. Kontrola adresního řádku se však vždy vyplatí.

<school specific> Jednotné přihlášení MUNI bude mít vždy podobu id.muni.cz. Každá, byť drobná změna webové adresy indikuje podvržený web. A nezapomeňte – obdržené podezřelé e-maily i již vyplněné phishingové formuláře vždy nahlašujte.

|  |
| --- |
| **Víte že...** pokusů o útok na principu spear-phishingu existuje celá řada? Ty nejzákeřnější nalezneme pod označením *business e-mail compromise* (BEC). Útoky BEC jsou charakteristické tím, že mají za cíl získat citlivé údaje od osob, které se v rámci hierarchického žebříčku firem zabývají nejčastěji činnostmi souvisejícími s penězi. Útočníci se v tomto případě vydávají za významné představitelé firem i VVŠ a pod maskou nadřízených rozesílají zaměstnancům podvodné e-maily s žádostí o uhrazení faktury po splatnosti či příkazu rychlého převodu peněz apod. Pachatelé často provádějí solidní množství průzkumů a pečlivě identifikují role ve společnosti. Zjišťují si, kdo jsou v dané společnosti účetní, manažeři, ředitelé... Dělají prostě vše pro to, aby obsah zaslaných e-mailů co nejvíce odrážel prostředí instituce na kterou cílí. |

## Smishing

**Radek, 47 let
STUDIJNÍ REFERENT**

Radek pracuje jako studijní referent na univerzitě již více něž 17 let, během této doby už se dobře naučil, že do e-mailové schránky občas přistávají zprávy, které mají nekalé úmysly. Proto si dává pozor a vzorně je nahlašuje. Co ale Radek netuší je, že útočníci se vyvíjejí a jejich útoky mohou cílit i na jiná zařízení. Dnes ráno totiž Radkovi přišla na služební telefon SMS zpráva, kde se psalo, že univerzitní covid-semafor přechází na červenou a ať se urychleně přes přiložený odkaz přihlásí do Informačního systému své univerzity a neprodleně obeznámí se situací všechny své kolegy na pracovišti. A co se v takové situaci stane? Úplně to samé jako u podvodného phishingového e-mailu, Radek dobrovolně odevzdal své údaje útočníkům, a ještě rozšířil poplašnou zprávu mezi své kolegy.

Tento typ útoku se nazývá Smishing. Jak i název napovídá, jedná se o phishing proveden prostřednictvím SMS zprávy. A může přijít i v mnohem atraktivnější formě, například doručovací SMS od dodávky jídla nebo jako výhra mobilního telefonu. Jak se této metodě sociálního inženýrství bránit?

Neposkytujte svá telefonní čísla na volně dostupných místech, pokud to není nutné. Na příchozí SMS zprávu neodepisujte a na dané číslo rozhodně nevolejte.

Neklikejte na přiložený odkaz v SMS zprávách dříve, než si ověříte identitu odesílatele, pokud je to možné. Ověření lze provést skrze sociální sítě, nebo můžete zkusit telefonní číslo zadat do prohlížeče a přečíst si recenze.

Máte-li podezření, že nemá příchozí zpráva zrovna nejčistší úmysly, neváhejte ji nahlásit svému zaměstnavateli, a v případě univerzity kompetentní osobě či přímo kyberbezpečnostnímu týmu.

## Vishing

**Markéta, 36 let
ČLENKA NADAČNÍHO FONDU**

Po náročném pracovním dni se Markéta konečně těšila na poklidnou chvilku čtení před spaním. V tu chvíli jí ale začal bzučet telefon s neznámým číslem svítícím na displeji. Markéta v rozhořčení hovor přijala, než ale stačila dotyčnému důrazně vysvětlit, že v takto pozdní hodinu je velmi nezdvořilé komukoliv volat, představil se jí profesionálně znějící hlas a začal na Markétu rychle naléhat. Byl prý napaden bankovní účet nadačního fondu, který spravuje, jedná se zásadní bezpečnostní problém a pro zajištění účtu potřebují o Markéty okamžitou spolupráci, ideálně aby pracovníkovi ihned sdělila přihlašovací údaje do bankovnictví, včetně PINU.

Markéta byla chvíli přirozeně zmatená a vyděšená, velmi rychle si ale uvědomila, že se musí jednat o podvodný telefonát, přihlašovací údaje se přeci nikdy nikomu nesdělují, natož PIN. Markéta měla pravdu, stala se totiž obětí Vishingu – voice-phishingu, tedy techniky podobné phishingu využívající ovšem pro přesvědčení oběti místo e-mailu podvodný hovor.

Hned jak si Markéta uvědomila, v jaké situaci se nachází, žádné údaje podvodníkovi nesdělila a hovor urychleně ukončila. Co bychom ale v podobné situaci my i Markéta měli dělat dál? V ideálním případě si poznamenat číslo, z kterého nám bylo voláno, čas, kdy nám bylo voláno a jaké údaje chtěl útočník vědět. S těmito údaji je vhodné se poté obrátit na policii, které mohou výrazně pomoci při dopadení pachatele a zabránění dalších podobných pokusů, které nemusí skončit tak dobře, jako Markétin příběh.

## Pretexting

**Lukáš, 19 let
NOVÝ STUDENT**

Začátek studia na univerzitě dokáže být extrémně stresující a takto ho také vnímá Lukáš, který nastupuje do prvního ročníku. Každý den mu chodí e-maily a upozornění, které ho informují o více i méně důležitých událostech z akademického světa, schránku postupně zaplavují všemožné pozvánky, instrukce a žádosti. Když tedy Lukášovi přišel e-mail, ve kterém ho “IT podpora MUNI” žádala o zaslání hesla do informačního systému pro ověření studentovy identity, zpočátku se nad ním příliš nepozastavoval, podobných starostí měl mnoho a přidal ho pouze na pomyslnou hromádku úkolů, které je potřeba splnit.

Když se pak ale k žádosti dostal podrobněji, uvědomil si, že sdělovat neznámému člověku, byť se podepíše jako správce systému, přes elektronickou poštu přístupové údaje, není v těchto situacích obvyklý postup. Zprávu si proto důkladněji prohlédl a při porovnání s jinými e-maily z univerzity zjistil, že adresa odesílatele má jiný tvar než obvykle, rozhodl se proto své údaje nezasílat.

Toto rozhodnutí Lukáše ochránilo před technikou sociálního inženýrství, kterou nazýváme Pretexting. Spočívá v tom, že si útočník vymyslí přesvědčivý příběh nebo scénář. Ten pak využívá při komunikací s vyhlédnutou obětí, kterou se snaží přesvědčit, aby spolupracovala a například, jako se tomu stalo v Lukášově případě, zaslala své přístupové údaje k různým účtům.

|  |
| --- |
| **Víte že...** pretexting může probíhat i ve fyzickém prostředí? Představte si následující situaci: přijdete na přednášku, posadíte se do zadních řad a otevřete si notebook. Za chvíli si k vám přisedne studentka, kterou osobně neznáte – ale zjevně chodíte na stejný předmět... Chvíli se zkouší přihlásit do sítě *eduroam* a za chvíli se obrátí na vás s tím, že se jí to nedaří a zda byste se nezkusili na jejím počítači přihlásit přes svoje údaje. Pomůžete jí? |

Důležité je proto mít na paměti, že své přihlašovací údaje a hesla bychom nikdy neměli nikomu zasílat ani sdělovat jakýmikoliv komunikačními prostředky. Nápomocné je také při každém podezření na nekalost kontrolovat adresu odesílatele v hlavičce e-mailu.

## Quid pro quo

**Tereza, 26 let
LABORANTKA**

Quid pro quo je technika, která může jednoduše nalézt své místo nejen v akademickém prostředí a jejíž důsledky málem zakusila laborantka Tereza. Tereza tráví mnoho času v laboratoři a svým experimentům a projektům je velice oddaná. Pečlivě si schraňuje data s nimi spojená a dbá o jejich bezpečnost, jelikož se mnohdy jedná o citlivé údaje. Jednoho dne jí ovšem přišla zpráva, ve které ji spřátelené výzkumné středisko žádá o zaslání dat z výzkumu, a to výměnou za peněžní odměnu. Středisko ve zprávě přesvědčivě argumentovalo, data prý plánuje využít pro rozšíření Terezina výzkumu o nové metody. Zasláním dat by tedy Tereza prý přispěla i k posílení vztahů mezi pracovišti, vzniku nových poznatků a rozvoji vědního oboru jako takového.

Přestože nabídka na první pohled zněla lákavě, Tereza si při čtení všimla podivné adresy, ze které zpráva přišla a brzy si uvědomila, že nejspíš obdržela podvodný e-mail a nejedná se o žádnou skutečnou žádost. Spojila se tedy skrze jiný komunikační kanál s údajným spřáteleným střediskem a skutečně – žádnou podobnou nabídku výzkumné pracoviště nezasílalo.

Ve skutečnosti si pouze na data brousil zuby útočník díky využití techniky Quid pro quo, která spoléhá na představení lákavé nabídky, často i se zmínkou finanční odměny. Tereze se ovšem v tomto případě díky zdravé obezřetnosti podařilo ochránit cenná výzkumná data před potenciálním zneužitím.

## Shoulder-surfing

**Kristýna, 21 let
STUDENTKA**

Nechybělo mnoho a Kristýna se stala obětí Shoulder Surfingu, metody sociálního inženýrství, která se vám může stát prakticky kdekoli a kdykoli. Shoulder Surfing, jak napovídá sám název, je založen na odpozorování důležitých dat a informací (například PINu) z displeje zařízení svého uživatele. Doslova tedy stačí, aby se vám útočník koukal přes rameno a čekal na správnou chvíli. I takto může začínat kybernetický útok a Shoulder Surfing může představovat jen jeden střípek z mozaiky.

Kristýna jednoho dne vyrazila městskou hromadnou dopravou do školy, jako téměř každý den, a rozhodla se zkontrolovat, jestli má v informačním systému již zapsanou známku za zkoušku. Tramvaj byla standardně přeplněná, ale Kristýna ukořistila místo k sezení. Když se přihlašovala, vůbec nezpozorovala podivného člověka za zády, kterému se přímo nabízel pohled do jejího přihlašovacího formuláře. Jak předejít podobné situaci?

Kristýna měla to štěstí, že zvolila dostatečně silné heslo, které nemohl útočník odpozorovat. Příště by měla ale dbát také na okolí a například si stoupnout zády ke stěně tramvaje, nebo ještě lépe využívat správce hesel, který heslo vyplní automaticky za ní. No a samozřejmě i zde platí, že pokud je to možné, měla by využívat 2FA (více viz modul 2).

|  |
| --- |
| **Pozor!** Minimalizujte manipulaci se svými citlivými údaji na veřejných místech. Internetové bankovnictví si raději zkontrolujte doma a pracovní e-maily jistě počkají do kanceláře. Stejně tak přihlašování do dalších univerzitních systémů a aplikací by mělo probíhat pouze v práci nebo s dostatečnou ochranou pro distanční přístup (např. VPN <school-specific: odkaz na návod>) - nikoliv například na veřejných WiFi v kavárnách. Problematické je také vyřizování pracovních věcí na cizím počítači či na počítači, kde je aktuálně přihlášen někdo jiný. |

Všechna tato doporučení platí nejen pro Shoulder Surfing, ale také pro ochranu vašeho soukromí jako takovou, a to i mimo kyberprostor. Soukromí bychom si všichni měli vždy pečlivě chránit.

## Sniffing

**Mikuláš, 47 let
PRACOVNÍK NAKLADATELSTVÍ**

Práce v univerzitním nakladatelství zahrnuje poměrně hodně papírování a korespondence, zejména pak na pozici marketingu a PR. Mikulášovi papírování nevadí, s čím si ale moc nerozumí, je nový e-mailový klient doporučovaný univerzitou. Uživatelské prostředí je pro něj neintuitivní, zbytečně komplikované a obecně nepřívětivé. Na internetu ovšem při brouzdání narazil na krásně vypadající aplikaci, která slibovala jednoduchý a mnohem přehlednější přístup k poště. A tak estetické prostředí! Mikuláš se zaradoval a aplikaci ihned nainstaloval na svůj pracovní počítač.

Na pracovním večírku se pak svým řešením pochlubil kolegovi z IT oddělení. Jaké bylo jeho překvapení, když mu kolega důrazně doporučil, aby aplikaci ihned odinstaloval a vrátil se ověřenému klientovi. Jednalo se totiž o aplikaci využívající zastaralý protokol pro stahování pošty, a tedy aplikaci náchylnou ke zneužití pomocí Sniffingu.

Při využití této techniky útočníci nasadí do sítě program, který dokáže “odposlouchávat” všelijaké informace, které sítí prochází. Podobným způsobem jako když policie v detektivkách napíchne telefonní linku, aby mohla následně dopadnout pachatele. Stejně jako v Mikulášově příběhu, při obraně proti Sniffingu se tedy jistě vyplatí poslechnout svého kolegu z IT a využívat vždy pro pracovní záležitosti ověřený software doporučený či zprostředkovaný samotnou univerzitou.

## Tailgating

**Michal, 28 let
VÝZKUMNÍK**

Že se sociální inženýrství a kybernetické útoky netýkají jen našich zařízení, e-mailových schránek nebo třeba serverů se dnes na vlastní kůži přesvědčí výzkumník Michal. Při rušném pondělním ránu Michal vchází do oddělení svého pracoviště, a sotva pípne kartičkou u vstupu, volá na něj pohledná mladá žena. „Pustíte mě prosím? Nechala jsem si kartičku doma.“ Michal prosbě gentlemansky vyhoví a slečně při vstupu ještě přidrží dveře. Na univerzitě pracuje pouhé dva měsíce, takže ještě nemá úplně přehled o všech svých spolupracovnících. Zatím ještě netuší, že slečnu už nikdy neuvidí...
Co Michal netuší zcela určitě je, že se právě stal obětí takzvaného Tailgatingu, který může mít nedozírné následky. Jak že se to mohlo stát?

Tailgating je metodou sociálního inženýrství, která využívá situace především ve velkých organizacích. Tato pracoviště často charakterizuje to, že se všichni zaměstnanci mezi sebou neznají. Hůře se jím tedy rozlišuje, kdo v tomto zázemí opravdu pracuje. A právě na to útočníci sázejí. Pro úspěch takového útoku pak stačí působit dostatečně sebejistě a v ideálním případě oběť rozptýlit. Jakmile se útočník dostane na pracoviště s omezeným přístupem, může způsobit spoustu potíží. Od ukradení dat z nezašifrovaného disku po nasazení škodlivého kódu do zařízení vedoucího pracovníka. Jak se proti Tailgatingu může Michal i vy bránit?

|  |
| --- |
| **Pozor!** Pokud se setkáte s někým, koho neznáte a tvrdí, že zapomněl ID kartu či klíče, pokuste se danou osobu prověřit například na vrátnici. Rozhodně ale nikdy nepouštějte neznámé osoby přímo na svá pracoviště. |

Pokud vstupujete do prostoru s omezeným přístupem, používejte vždy pouze své identifikační karty a klíče. Zároveň je nikdy nezapůjčujte jiným osobám, a to ani kolegům. A na závěr k zamyšlení –nepouštěli jste v poslední době někoho cizího na své pracoviště?

## Trashing

**Lenka, 43 let
MZDOVÁ ÚČETNÍ**

Lenka, která pracuje na personálně-mzdovém oddělení při úřadu většího města, nastoupila do nové práce před třemi měsíci. Minulý týden se jí do denní agendy dostal úkol – vystavit zápočtový list zaměstnanci, který odchází. Lenka tedy vše připravila, ale při předání si zaměstnanec všimnul drobného překlepu ve svém příjmení. Lenka tedy připravila nový zápočtový list a ten starý hodila v rychlosti do koše. Za pár dnů začala kopie tohoto zápočtového listu putovat po internetu. Ukázalo se, že zápočtový list obsahuje velmi citlivé údaje, které by nikdo z nás nechtěl veřejně sdílet. Například, jestli se ze mzdy prováděly nějaké soudem nařízené srážky.

Co se tedy stalo? Lenka okamžitě dostala podezření na škodlivý software ve svém počítači. Vysvětlení je však mnohem více prosté. Takzvaný Trashing je technika sociálního inženýrství, kde útočník zkouší získat informace mezi vyhozeným smetím z kanceláří. Ano, čtete správně. Takto se zápočtový list dostal na internet, odkud už ho pravděpodobně nikdy nikdo nesmaže. Jak se tedy bránit proti Trashingu?

Nejúčinnější metodou je prevence. Útočníci dokážou být velmi obratní při pokusech o získání citlivých údajů a informací, zvlášť jedná-li se o vytipovanou oběť.

Pamatujme tedy, že odpadkové koše nejsou černé díry. I v případě, kdy dokument jen ručně roztrháte nebo rozstříháte, obratný útočník si poradí. Svěřte tedy nepotřebné dokumenty raději skartovačce.

**A na závěr...**

Techniky sociálního inženýrství mohou být v kyberprostoru – a částečně i mimo něj – každodenní hrozbou pro každého. Některé možné scénáře jsme vám představili, jejich hlavní účel ale spočívá v názorných ukázkách, jak kreativní útočníci dokážou být a také, že nikoho nešetří. Pojďme si to celé shrnout. Toto jsou základní kroky, jak se preventivně bránit před technikami sociálního inženýrství, které lze snadno aplikovat do našeho každodenního života:

|  |
| --- |
| **Na co nezapomenout ze čtvrtého modulu?**Vždy ověřujte adresu odesílatele zprávy a adresní řádek na webu (více v modulu 3).Neotvírejte e-maily a přílohy z podezřelých zdrojů.Mějte nainstalován antivirový program a udržujte jej aktualizovaný.Nikdy nezapojujte a nevkládejte externí nosiče, u kterých si nejste jisti původem a obsahem.Minimalizujte manipulaci se svými citlivými údaji na veřejných místech.Nepůjčujte své identifikační karty a klíče žádným osobám, dokonce ani kolegům. |

|  |
| --- |
| **Pozor!** **Co dělat, když se něco pokazí?** V případě, že došlo k bezpečnostnímu incidentu nebo máte podezření, že mohlo být narušeno vaše kyberbezpečí, obracejte se na <school-specific: doplňte kontaktní osobu nebo popište proces řešení kyberbezpečnostních incidentů>. |